

1 CLAIMS

2 We claim:

- 3 1. A Video-on-Demand method for demanding a video program via a short
4 message, comprising the steps of:
5 generating, at a user end, a demand short message including information on the
6 demanded video program, said demand short message including at least a User Identifier
7 field, a Program Identifier field of the demanded video program and an Authentication
8 field;
9 sending to a program delivering end the generated demand short message;
10 receiving the demand short message at the program delivering end, and processing
11 the received demand short message to extract a user identifier and using the
12 Authentication field to authenticate legality of the user;
13 after authenticating the legality of the user successfully, sending program content
14 corresponding to a program identifier from the program delivering end to the user end
15 indicated by the user identifier; and
16 receiving the demanded video program at the user end.
- 17 2. A Video-on-Demand method according to claim 1, further comprising the step of
18 sending from the program delivering end to the user end a reply message including a
19 confirmation message indicating that the demand short message has been received.
- 20 3. A Video-on-Demand method according to claim 1, further comprising the steps of:
21 encrypting the fields in the generated demand short message except the
22 Authentication field at the user end, and
23 decrypting the received encrypted short message at the program delivering end to
24 extract the user identifier and the program identifier.

1 4. A Video-on-Demand method according to claim 1, wherein said demand short
2 message further comprising:
3 a Format Identifier field for defining a format of said demand short message;
4 a Demand Time field for indicating a time for sending said demand;
5 a Playback Time field for indicating a start time of video playing;
6 an Optional field containing optional data that may describe said demand more
7 precisely; and
8 said Authentication field is an encrypted digest of the above User Identifier field,
9 Program Identifier field, Format Identifier field, Demand Time field, Playback Time field,
10 and Optional field.

11 5. A Video-on-Demand method according to claim 4, wherein said Authentication field is
12 generated according to the following procedure:
13 calculating the digest of all the fields except the Authentication field using a
14 digest algorithm;
15 encrypting with a cipher algorithm a calculated digest by adopting a secret
16 authentication key corresponding to a user end device, uniquely allocated in
17 advance by the program delivering end; and
18 a process of authenticating a user's legality by the program delivering end being
19 conducted according to the following procedures:
20 calculating the digest of all the fields except the Authentication field using
21 a digest algorithm;
22 encrypting with a cipher algorithm the calculated digest by adopting a
23 secret authentication key corresponding to a user end device, uniquely
24 allocated in advance by the program delivering end, so as to calculate an
25 Authentication field; and
26 checking whether the calculated Authentication field and the received
27 Authentication field are identical.

- 1 6. A Video-on-Demand method according to claim 5, wherein when said video program
2 is sent via a conditional access system, a content key is delivered with the video program,
3 so there is no need for a separate deliver of said reply message.
- 4 7. A Video-on-Demand method according to claim 5, wherein when the video program
5 demanded by the user needs to be encrypted and the encrypt key is not sent via a
6 conditional access system, the method further comprising the steps of:
7 generating, at the program delivering end, an encrypted reply message containing a
8 content key of said video program, and sending it to the user end;
9 decrypting, at the user end, the content key from said encrypted reply message; and
10 decrypting the video program received from the program delivering end according
11 to the decrypted content key.
- 12 8. A Video-on-Demand method according to claim 7, wherein said encrypted content key
13 is encrypted using a device key corresponding to the user end device, uniquely allocated
14 in advance by the program delivering end, and said device key can be different from said
15 Authentication key.
- 16 9. A Video-on-Demand system for demanding a video program via a short message,
17 comprising:
18 short message generating means for receiving a user demand, and generating a
19 demand short message based on the user demand, said demand short message including at
20 least a User Identifier field, a Program Identifier field of the demanded video program and
21 an Authentication field;
22 short message sending means for sending the demand short message generated by
23 the short message generating means;
24 demand short message processing means at a program delivering end for receiving
25 the demand short message, processing the received demand short message to extract the
26 user identifier and using the Authentication field to authenticate the legality of the user,

1 and sending the program identifier of the demanded program by a legal user to video
2 delivering means;

3 video delivering means for sending program content corresponding to the program
4 identifier from the program delivering end to the user end indicated by a legal user
5 identifier; and

6 program playing means at the user end for receiving the video program sent by the
7 video delivering means and playing it back to the user.

8 10. A Video-on-Demand system according to claim 9, wherein the demand short message
9 processing means further comprises a reply message generating unit for generating a reply
10 message including at least a confirmation message indicating that the demand short
11 message has been received, for sending to the user end.

12 11. A Video-on-Demand system according to claim 9, wherein:

13 the short message generating means further comprises an encrypting unit for
14 encrypting the fields in the generated demand short message except the Authentication
15 field; and

16 the demand short message processing means further comprises decrypting means
17 for decrypting the received encrypted short message.

18 12. A Video-on-Demand system according to claim 9, wherein said short message
19 generating means further comprises a program information generating unit for generating
20 said User Identifier field, said Program Identifier field of the video program demanded by
21 the user and

22 a Format Identifier field for defining a format of said demand short message,
23 a Demand Time field for indicating a time for sending said demand,
24 a Playback Time field for indicating a start time of video playing, and
25 an Optional field containing optional data that may describe said demand more
26 precisely.

1 13. A Video-on-Demand system according to claim 12, wherein
2 said short message generating means further comprises an Authentication field
3 generating unit for calculating a digest of all the fields except the Authentication field
4 using a digest algorithm and encrypting with a cipher algorithm the calculated digest by
5 adopting a secret authentication key corresponding to a user end device, uniquely
6 allocated in advance by the video delivering means; and
7 said demand short message processing means further comprises an authentication
8 unit for calculating the digest of said User Identifier field, Program Identifier field,
9 Format Identifier field, Demand Time field, Playback Time field and Optional field,
10 encrypting with a cipher algorithm the calculated digest by adopting a secret
11 authentication key corresponding to a user end device, uniquely allocated in advance by
12 the video delivering means, so as to calculate an Authentication field and checking
13 whether the calculated Authentication field and the received Authentication field are
14 identical.

15 14. A Video-on-Demand system according to claim 13, wherein if said video program is
16 sent via a conditional access system, a content key is delivered with the video program.

17 15. A Video-on-Demand system according to claim 13, wherein if the video program
18 demanded by the user needs to be encrypted and the encrypt key is not sent via a
19 conditional access system, then
20 the demand short message processing means generates an encrypted reply message
21 containing a content key of said video program, and sends it to the user end; and
22 the program playing means at the user end decrypts the content key from said
23 encrypted reply message, and decrypts the video program received from the program
24 playing means according to the decrypted content key.

1 16. A Video-on-Demand system according to claim 15, wherein said encrypted content
2 key is encrypted using a device key corresponding to the user end device, uniquely
3 allocated in advance by the program delivering end, and said device key can be different
4 from said Authentication key.

5 17. Short message generating means in a Video-on-Demand system, comprising:
6 a receiving unit for receiving a user demand;
7 a program information generating unit for generating, according to the user
8 demand, program information including at least a User Identifier field and a Program
9 Identifier field of the demanded video program;
10 an Authentication field generating unit for generating a Authentication field
11 according to the program information generated by the program information generating
12 unit; and
13 an output unit for outputting said program information and the Authentication field
14 as a demand short message to short message sending means.

15 18. A short message generating means according to claim 17, further comprising:
16 an encrypting unit for encrypting the fields except the Authentication field in the
17 demand short message.

18 19. A short message generating means according to claim 17, wherein said program
19 information generating unit further generating:
20 a Format Identifier field for defining a format of said demand short message,
21 a Demand Time field for indicating the time for sending said demand,
22 a Playback Time field for indicating the start time of video playing, and
23 an Optional field containing optional data that may describe said demand more
24 precisely.

25 20. A short message generating means according to claim 19, wherein

1 said Authentication field generating unit calculates the digest of all the fields
2 except the Authentication field using a digest algorithm and encrypts with a cipher
3 algorithm the calculated digest by adopting a secret authentication key determined in
4 advance and uniquely corresponding to said short message generating apparatus.

5 21. A short message generating means according to claim 20, wherein said digest
6 algorithm is MD5 algorithm, and said cipher algorithm is 3DES algorithm.

7 22. A short message generating method in a Video-on-Demand system, comprising the
8 steps of:

9 receiving a user demand;

10 generating, according to the user demand, program information including at least a
11 User Identifier field and a Program Identifier field of a demanded video program;

12 generating an Authentication field according to the generated program information;

13 and

14 outputting said program information and the Authentication field as a demand short
15 message to short message sending means.

16 23.. Demand short message processing means in a Video-on-Demand system,
17 comprising:

18 a receiving unit for receiving a demand short message;

19 an extracting unit for extracting a user identifier from the demand short message
20 received by the receiving unit;

21 an authentication unit for authenticating legality of a user identified by the user
22 identifier extracted by the extracting unit, according to the Authentication field in the
23 demand short message received by the receiving unit; and

24 an outputting unit for outputting a program identifier of the program which the
25 legal user demands.

- 1 24. A demand short message processing method in a Video-on-Demand system,
2 comprising the steps of:
3 receiving a demand short message;
4 extracting a user identifier from the received demand short message;
5 authenticating legality of a user identified by the extracted user identifier, according
6 to the Authentication field in the received demand short message; and
7 outputting a program identifier of the program which the legal user demands.
- 8 25. An article of manufacture comprising a computer usable medium having computer
9 readable program code means embodied therein for causing Video-on-Demand, the
10 computer readable program code means in said article of manufacture comprising
11 computer readable program code means for causing a computer to effect the steps of
12 claim 1.
- 13 26. A program storage device readable by machine, tangibly embodying a program of
14 instructions executable by the machine to perform method steps for Video-on-Demand,
15 said method steps comprising the steps of claim 1.
- 16 27. A computer program product comprising a computer usable medium having
17 computer readable program code means embodied therein for causing
18 Video-on-Demand, the computer readable program code means in said computer program
19 product comprising computer readable program code means for causing a computer to
20 effect the functions of claim 9.
- 21 28. A computer program product comprising a computer usable medium having
22 computer readable program code means embodied therein for causing short message
23 generation, the computer readable program code means in said computer program product

1 comprising computer readable program code means for causing a computer to effect the
2 functions of claim 17.

3 29. An article of manufacture comprising a computer usable medium having computer
4 readable program code means embodied therein for causing short message generation, the
5 computer readable program code means in said article of manufacture comprising
6 computer readable program code means for causing a computer to effect the steps of
7 claim 22.

8 30. A program storage device readable by machine, tangibly embodying a program of
9 instructions executable by the machine to perform method steps for short message
10 generation, said method steps comprising the steps of claim 22.

11 31. A computer program product comprising a computer usable medium having
12 computer readable program code means embodied therein for causing short message
13 generation, the computer readable program code means in said computer program product
14 comprising computer readable program code means for causing a computer to effect the
15 functions of claim 23.

16 32. An article of manufacture comprising a computer usable medium having computer
17 readable program code means embodied therein for causing demand short message
18 processing, the computer readable program code means in said article of manufacture
19 comprising computer readable program code means for causing a computer to effect the
20 steps of claim 24.

21 33. A program storage device readable by machine, tangibly embodying a program of
22 instructions executable by the machine to perform method steps for demand short
23 message processing, said method steps comprising the steps of claim 24.